Password Procedure

Section 1 - Purpose

(1) This Procedure sets out Charles Sturt University's standards regarding Password and Personal Identification Number (PIN) management (including strength, quality, creation, protection, storage, re-use and re-setting) and maintenance.

(2) Passwords are the primary authentication credential used by Charles Sturt University's Information and Communication Technology (ICT) systems to verify the identity of individuals wanting to gain authorised access to ICT systems.

(3) Poor choice of passwords or poor password management may present unacceptable risk to staff, student and University information in the form of unauthorised disclosure or loss of integrity or information availability.

Scope

(4) This Procedure applies to all users including staff, students, visitors and associates of Charles Sturt University (the University) who:

a. create and manage Passwords and/or PINs used to access the University's ICT systems for official University purposes;
b. are responsible for managing a University ICT system account that supports or requires Passwords or PINs to access; and
c. are responsible for systems that manage, transport and store University credentials used by individuals.

References

(5) This Procedure should be read in conjunction with:

a. Information and Communications Technology Security Policy;
b. Australian Government Department of Defence Information Security Manual 2016 Controls;
c. Australian Access Federation Assurance Framework;
d. Computing and Communications Facilities Use Policy;
e. Data Security Classification Scheme;
f. Student Misconduct Rule 2020; and
g. Code of Conduct.

Section 2 - Glossary

(6) For the purpose of this Procedure:

a. Budget Centre Manager - means the staff member with authority for a defined budget centre. Refer to the Delegations and Authorisations Policy;

b. Applications Portfolio - means the University's official register of application assets;
c. Expired Password - means a password that cannot be used to authenticate because it has not been changed within the specified timeframe;
d. Multi-factor Authentication - means the use of more than one authentication method for access to an application or system;
e. Password - means a confidential string of characters used by individuals to allow access to a computer, ICT interface or system;
f. Personal Identification Number (PIN) - means a secret number (usually four to six digits in length) known only to an individual. Used to confirm identity and gain access to an ICT system;
g. Privileged Account - an account used by individuals or systems to access application or ICT system administrative or higher level functions than that of a user account;
h. Privileged Password - means an additional Password used by individuals or systems to authenticate access to administrative or higher level functions of an application or ICT system;
i. Role Management - means the mechanism by which an application manages the functions a User can perform and the data which a User has access to within the application;
j. Service Account - an account that an application or service uses to interact with an operating system, database or integration service and cannot be used for User or Privileged account functions;
k. Service Account Password - means a Password used by an account that an application or service uses to interact with an operating system, database or integration service and cannot be used for User or Privileged account functions;
l. System or Application Custodian - means executive staff with recognised responsibility and ownership of University information or ICT assets as identified in the CSU Application Portfolio; or for non-registered systems, the primary Budget Centre Manager that has established the non-registered system;
m. User - means staff, students, vendors, visitors, partners and associates of the University who access University ICT systems and services;
n. Username - means a unique series of characters used to identify a user to allow access to a computer, ICT interface or system. Username is also sometimes referred to as login name;
o. User Account - refers to the arrangement through which a user is given personalised access is organised to a computer, ICT interface or system; and
p. User Password - means a Password held by an individual to authenticate standard user access to a University application or ICT system.

Section 3 - Policy

(7) Refer to the Information and Communications Technology Security Policy.

Section 4 - Procedures

Responsibilities

(8) The Division of Information Technology (DIT) is responsible for the provisioning, storage and management of centralised password datasets used for authentication to applications and ICT services listed in the University's Applications Portfolio.

(9) Users are responsible for:

a. Password creation, use and management, associated with University credentials; and

b. Reporting any actual or suspected Password compromises to the IT Service Desk Request if staff or Student Central if a student.

(10) Application Custodians of systems not listed in the University's Applications Portfolio or not using centralised authentication systems are required to comply with this Procedure regarding the provisioning, storage and management of password datasets used for authentication.

(11) Exemptions to this Procedure must be approved in writing from the Executive Director, Division of Information Technology.

(12) At the discretion of the Executive Director, Division of Information Technology, ICT systems that do not comply with this Procedure may be removed from operation until compliance can be demonstrated or exemption approved.

Password Strength

(13) All Passwords are classified as Highly Confidential as per the University's Data Security Classification Scheme.

(14) User Password strength and complexity is based on the minimum requirements as defined by the Australian Access Federation Assurance Framework - Level 2.

(15) All User Passwords must be at least eight characters in length consisting of at least three of the following:

a. lowercase alphabetic characters (a-z);
b. uppercase alphabetic characters (A-Z);
c. numeric characters (0-9); or
d. special characters ($%#).

(16) Privileged and Service Account Password strength and complexity are based on the requirements as defined in the Australian Government Department of Defence Information Security Manual 2016 Controls.

(17) All Privileged and Service Account Passwords must be at least eleven characters in length consisting of at least three of the following:

a. lowercase alphabetic characters (a-z);
b. uppercase alphabetic characters (A-Z);
c. numeric characters (0-9); or
d. special characters ($%#).

(18) Passwords as part of Multi-factor Authentication must be a minimum of six alphabetic characters with no complexity requirement.

(19) Passwords must be difficult to guess and not be a single dictionary word.

(20) Passwords must not be the same as, or a variation of, the associated Username.

(21) Personal Identification Numbers (PIN) must be difficult to guess and not a repetition of the same digit.

(22) Passwords must be unique and not the same as Passwords used for non-University accounts such as personal social media accounts, personal emails accounts and online banking.

(23) ICT systems must be configured to enforce complexity and dictionary strength requirements.

(24) When ICT systems cannot be configured to enforce Password strength requirements, Passwords must be checked

by alternative means to ensure compliance with this Procedure.

(25) Upon consultation with and approval from DIT, alternate authentication mechanism that do not use passwords or pin numbers may be used (e.g. biometric authentication, tokens, or certificates).

Password Changing

(26) To minimise disruption to services, Passwords should be changed prior to Password expiry.

(27) User Passwords must expire after 120 days.

(28) Privileged Passwords must expire after 90 days.

(29) Service Account Passwords must expire after 180 days.

(30) There is no Password expiry requirement for students, excepting those students who are Higher Degree Research (HDR) students with access to additional services and/or those who are also staff members. For these students User Password expiry requirements outlined in this Procedure apply.

(31) Passwords must not be re-used for six consecutive changes.

(32) Passwords cannot be changed by the authorised user more than twice a day.

Password Use and Storage

(33) Passwords and PINs are only to be used by an individual and must not be:

a. shared with anyone under any circumstances; or
b. written down or recorded in physical or clear text electronic format.

(34) If the confidentiality of a Password or PIN is in doubt, it must be changed immediately.

(35) If the confidentiality of a Password or PIN has been compromised, DIT will:

a. lock the associated account;
b. advise the credential holder; and
c. manage the associated risk.

(36) The use, storage and/or transport of plain text Passwords is prohibited.

(37) Authentication systems must not store Passwords or PINs in a viewable or recoverable format.

(38) A record of all credential registration, history, status and revocation must be kept for seven years and six months after expiration or revocation (whichever is later).

Applications and Systems

(39) To facilitate compliance with this Procedure, the University's applications and systems must utilise centralised enterprise authentication systems where practical.

(40) Forgotten, expired or locked-out Passwords must be re-set and not recovered.

(41) Authentication mechanisms must disable User and Privileged Accounts for a period of 30 minutes after five consecutive failed authentication attempts and notify the account holder.

(42) Authentication mechanisms must disable and notify the owner of Service Accounts after two consecutive failed authentication attempts.

(43) Authentication mechanisms involving the use of passwords must use secure, strong encryption protocols in the transport of credential information.

(44) Applications must provide role management to allow one user to undertake the functions of another without the need to share Passwords.

(45) Failure to comply with this Procedure that occurs as a result of deliberate, malicious or negligent behaviour may result in disciplinary action as per the University's misconduct process.

Section 5 - Guidelines

(46) Nil.

Status and Details

Status	Historic
Effective Date	27th October 2017
Review Date	28th October 2019
Approval Authority	Chief Financial Officer
Approval Date	26th October 2017
Expiry Date	3rd December 2020
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Philip Roy
Enquiries Contact	Division of Information Technology